UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/032,722	10/27/2001	Shigeki Kamiya	450100-03253.1	6409

20999 7590 11/30/2007

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
11/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/032,722	KAMIYA ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3,8,13,18,23 and 26-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3,8,13,18,23 and 26-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 9/20/2007.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/20/2007 has been entered.

Response to Arguments

Applicant's arguments with respect the claims have been considered but are not found persuasive.

Regarding applicants' argument that the combination of Rosner, Kato, and Schneier do not disclose "generating a set of passkeys specific to each destination", the examiner does not find the argument persuasive. After further consideration of the teachings of Rosner, the examiner is now relying on the "partial keys" X1-X4 and the group key X. Because each of X1-X4 is for use by each of the recipients respectively, the set is specific to each of the recipients. As such, the examiner does not find the argument persuasive.

Regarding applicants' argument that Rosner, Kato and Schneier do not disclose "generating a plurality of partial keys based on a portion of the passkeys", the examiner does not find the argument persuasive. In the combination relied upon by the examiner, as shown below, it would be obvious to create "key parts" from each of the partial keys X1-X4, as Schneier

teaches splitting keys and transmitting each of the key parts over a different channel. As such, the examiner does not find the argument persuasive.

Regarding applicants' argument that Schneier does not teach splitting of keys, the examiner does not find the argument persuasive. The claims do not require "splitting keys". Rather, the claims require dividing keys. The applicants admit on page 10 Lines 12-14 that section 3.6 of Schneier teaches dividing a message, but the applicants continue to argue that the message is not a key. However, Page 177 of Schneier states with regards to key distribution, that "another solution...splits the key into several different parts (see **Section 3.6**)". It is clear that Schneier is teaching that the message dividing method of 3.6 should be used to split (or divide) a key for key distribution. Therefore, the examiner does not find the argument persuasive.

Regarding applicants' argument that Schneier teaches away from dividing an encryption key by a division pattern, the examiner does not find the argument persuasive. First, as discussed above, Schneier does in fact disclose dividing keys. Second, Schneier does teach the use of a "division pattern". The examiner is relying on the random-bit strings of Schneier as meeting the limitations of the division pattern of claims 26-29. As such, the examiner does not find the argument persuasive.

Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25 have been examined.

All objections and rejections not presented below have been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter

sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 8, 13, 18, and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosner et al. (US Patent Number 6,636,968) hereinafter referred to as Rosner, and further in view of Kato (US Patent Number 6,381,331), and further in view of Schneier ("Applied Cryptography").

Regarding claim 3, Rosner disclosed a digital data delivery method for use in delivering digital data from an upstream system to a downstream system, said upstream system providing multipoint delivery of encrypted digital data to specific destinations, and said downstream system decrypting the delivered digital data (See Rosner Fig. 4 and Col. 4 Paragraph 3), said method comprising the steps of: encrypting digital data by said upstream system using an encryption key (See Rosner Col. 3 Lines 42-45); generating on the basis of said encryption key (K), a set of passkeys specific to each of said specific destinations (X, X1, X2, X3, X4) by dividing said encryption key by a division pattern (X^{y1} or X^{y2} or X^{y3} or X^{y4}) unique to each of said specific destinations (See Rosner Fig. 3 Box 210, the abstract, and Col. 4 Line 36 - Col. 5 Line 7 wherein X1 is equivalent to K / (X^{y1}), and similarly X2 is equivalent to K / (X^{y2}), and so on for X3 and X4, as can be seen in Fig. 4 Equation 450); and delivering the passkeys to each of said specific destinations (See Rosner Col. 5 Lines 8-13); delivering the encrypted digital data (See Rosner Col. 5 Lines 8-13); restoring said encryption key by using said downstream system using said passkeys (See Rosner Col. 5 Lines 13-38); and using the restored encryption key to

decrypt the encrypted digital data (See Rosner Col. 5 Lines 28-33), but Rosner failed to disclose that said division pattern based on the content of said digital data; or generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information from which said passkeys may be reproduced; or delivering either said plurality of partial keys or partial key information, from which said partial keys may be reproduced, and delivering the remaining passkeys not used to generate said partial keys or the remaining passkey information, to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other; or restoring said encryption key by using said downstream system using either said plurality of partial keys or said partial key information and using either said remaining passkeys or said remaining passkey information delivered over said plurality of delivery routes.

Kato teaches that in an content sending system, in order to prevent the content from being repetitively gotten without approval, the encryption keys used to encrypt the content should be prepared for each content (See Kato Col. 10 Lines 37-52).

Schneier teaches that key information should be delivered over a different communication channel than the data encrypted using the key information (See Schneier Col. Page 176 Lines 34-37). Schneier further teaches that keys should be split and each part should be delivered over a separate channel (See Schneier Page 177 Paragraph 1). Schneier further teaches that the key should be split using random numbers, which would be unique for each splitting (See Schneier Pages 70-71 Section 3.6 Secret Splitting).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kato in the delivery system of Rosner, by providing each

content with its own encryption key (K). This would have been obvious because the ordinary person skilled in the art would have been motivated to prevent a recipient from decrypting multiple contents without approval. In this combination, a new division pattern (X^{yi}) would be created as taught by Rosner regarding the creation of the encryption key K (See Rosner Col. 4 Lines 36-53).

It further would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the partial key delivery system of Rosner by splitting and delivering the partial keys (X1, X2, X3, and X4) and group key (X) used to reconstruct the decryption key over different channels and further over a different channel than the encrypted content, and to restore said encryption key by using said downstream system using the plurality of split keys and using the split group key (remaining passkey information) delivered over said plurality of delivery routes. This would have been obvious because the ordinary person skilled in the art would have been motivated to further protect the key from being illicitly reconstructed as well as to protect the encrypted content from being illicitly decrypted.

Claims 8, 13, and 18, are rejected for the same reasons as claim 3 above and further because Rosner disclosed the upstream system (See Rosner Fig. 2 Element 210).

Regarding claims 26-28, Rosner, Kato, and Schneier taught that a set of said partial keys is generated by dividing a portion of said set of passkeys specific to a destination by a predetermined division pattern specific to the destination of said set of partial keys (See Schneier Section 3.6 and Page 177 Paragraph 1).

Claims 23, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Rosner, Kato, and Schneier as applied to claim 3 above, and further in view of Schneier.

The combination of Rosner, Kato and Schneier disclosed a system and method for communicating encrypted data using key reconstruction at the receiver (See the rejections of claims 1-5 above), but failed to disclose software for implementing the method.

Schneier teaches that any encryption algorithm can be implemented in software (See Schneier Page 225 Lines 25-38).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the encryption system of Rosner and Schneier by providing software to implement the encryption method. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide flexibility and portability, ease of use, and ease of upgrade to the encryption system.

Regarding claim 29, Rosner, Kato, and Schneier taught that a set of said partial keys is generated by dividing a portion of said set of passkeys specific to a destination by a predetermined division pattern specific to the destination of said set of partial keys (See Schneier Section 3.6 and Page 177 Paragraph 1).

Conclusion

Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

/Matthew Henning/
Assistant Examiner
Art Unit 2131
11/27/2007